

FIREWALL POOLING IN A NETWORK FLOWSWITCH

Srinivas Chaganty

Makarand Kale

Satish Bommareddy

Abstract

A firewall fault tolerant network interface system includes a switch circuit configured to detect when a firewall fails in a multi-firewall local network. When a failed firewall is detected, the switch circuit waits for a time-out period to expire to allow convergence. The switch circuit then intervenes when traffic from a server to the failed firewall is detected. The switch circuit translates the MAC address of the failed firewall to the MAC address of a functional firewall. Traffic from a server originally directed to the failed firewall is then redirected to a functional firewall. In a further refinement, the switch circuit provides the MAC address of a functional firewall in response to an ARP request from a server to the failed firewall. Thus, traffic from this server will be directed to the functional firewall without further intervention, reducing the overhead of the switch circuit. In still a further refinement, if the failed firewall recovers, the switch circuit waits for a time-out period to expire to allow convergence of external firewalls and to allow the recovered firewall to learn routes to known clients. The switch circuit then ceases all intervention for the MAC address of the now recovered firewall.